P.p1 al 2004, william 2003, bishop 2003,

p. p1 {margin: 0. 0px 0.

0px 0. 0px 0. 0px; text-align: justify; font: 12.

0px ‘ Times New Roman’; -webkit-text-stroke: #000000} p. p2 {margin: 0. 0px 0. 0px 0. 0px 0.

0px; text-align: justify; font: 12. 0px ‘ Times New Roman’; -webkit-text-stroke: #000000; min-height: 15. 0px} span. s1 {font-kerning: none} span.

Apple-tab-span {white-space: pre} Basically, what the biometric does is, it requires an individual to be physically present. Whereas with a password, you can easily provide that to someone else. – LARRY HORNAKAn authentication system that uses old method usually have some weaknesses, because it is easy to forget the passwords or PINs of ATMs, Smart cards, Computer networks, and etc (Kaufman et al, 2002). Moreover, using the old method increases the probability of criminal activity to happen, for example someone who knows your password and uses it for criminal purpose. Biometrics technology is one promising solution to face this problem, based on “ what we are” and “ how we behave” (El-Abed, Charrier, 2014: 150). This technology works automatically based on our biological identity. There are two types of biometrics technology based on physiological appearance and behaviour. From physiological such as face recognition, hand geometry, fingerprint, iris, retina, ear recognition.

Then, from our behavioural such as voice, signature, gait, keystroke dynamics, lips movements. In addition, biometric technology should be use and apply in our daily life, because it increases security and privacy,

authenticity and accuracy, effectiveness and is easy to use. Biometric technology is one of the tools that can increase our security and privacy. The development of technology also increases the rate of cybercrime, such as identity fraud, data theft, hacking, password vulnerability, denial of service, sabotage and etc. For instance, a recent survey that is reported by Boroshok (2005) proves that 71% of the US consumers would pay more for biometric security option in their cell phones and 63% to be added to their personal computers since the 911 attack.

This shows that biometric technology prevent the rate of crime. Because of that, many researchers have proposed the use of biometric based authentication as secure and private way to access data on the network. Haag et al 2004, William 2003, Bishop 2003, Ann et at 2007, Umit 2006. From that authentication system, there are a lot of methods to identify and the purposes of this technology are for security and privacy. It had been proven by researchers from Japan researched the usage of fingers prints, they identified the percentage of the success rate at the range of about 67-100% using biometric technology (Matsumoto, Matsumoto et al, 2002).

Based on Matsumoto research, this method is highly recommended because it can prevent the rate of crime. Biometric technology is one of the tools that can increase authenticity and accuracy. In China during the 14th century, finger prints method was already invented. They used ink to take the fingerprints.

The purpose of this method is to check the authentication for identification. In 1890, Alphonse Bertillon used that method to identify criminals

(Bhattacharyya, Ranjan, A. Farkhod, Choi, 2009: 14). Nowadays, biometrics for authentication is growing and also have law regulations to check the authentication and calculate accurately for security and privacy. According to Andrew S. Patrick (2008), there are four main measures of biometrics accuracy True Match Rate (TMR), False Match Rate (FMR), True Non-Match Rate (TNMR), False Non-Match Rate (FNMR). These measures of biometric accuracy interconnected in biometric systems, there is a mathematical relationship between the corresponding true and false rates, and there is inevitably a trade-off where attempts to minimize the false matches of a system tend to decrease the frequency of true matches (Patrick S, 2008).

In addition, there are also three other measures that can supports of biometric accuracy, such as False accept rate (FAR), False reject rate (FRR), Failure to enroll rate (FTE) (Sasidhar, Kakulapati, Ramakrishna, KailasaRao, 2010). So, it is difficult for people who want to manipulate our physiological or biological appearance because there isn’t a authenticate tools they can use. Biometric technology is one of the tools that can increase effectiveness and is easy to use. Because we just use our physiological or behavioural to be identified. The example of biometric technology in our daily life are finger prints in our smartphone for security, a fingerprint for attendance, and etc. Biometric technology is built from modern systems and is designed to be easy and safe to use. This technology also saves time, so it is more effective, more productivity and decline costs cheaper by eliminating fraud and waste.

There is an example from Federal Bureau of Investigation (FBI), There is an example from Federal Bureau of Investigation (FBI), they used the fingerprint

biometric technology for criminal investigations (Saini M, Kapoor AK, 2016). According to M. Saini and AK Kapoor (2016) The Integrated Automated Fingerprint Identification System (IAFIS) is a national automated system that used fingerprint biometrics technology, that has control by FBI for identification and criminal history. As stated before, IAFIS gives automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses. IAFIS already have 70 million subjects in the criminal master file, 31 million civil prints, fingerprints from 73, 000 known and presumed as terrorists that are handled by the U.

S. or by international law enforcement agencies. The common response time using electronic criminal fingerprint submission is about 27 minutes.

Whereas, electronic civil needs an hour and 12 minutes to handle the submissions (Saini M, Kapoor AK, 2016). It is proven that by using the tools of biometric technology more effective and waste less time. As stated before, first, we can use biometric technology to protect us from criminal activity as a security. Therefore, we must increase our security by using biometric technology, because the development of technology also increases the rate of cybercrime. Second, biometric technology is one of the tools that can check the authentication and measure or calculate something accurately. So it can help us to minimise the erroneous or mistake. Last, biometric technology is also easy to use, because it is based on “ what we are” and “ how we behave”.

We just use our physiological appearance and behaviour. Biometrics technology is also built from modern systems and is designed to be easy and safe to use. Beside of that, it can save our time, because biometric technology is more effective than the conventional method. It is important for us to use this technology because it has many benefits for us. Therefore, we should use and apply biometric technology in our daily life.